REMARKS

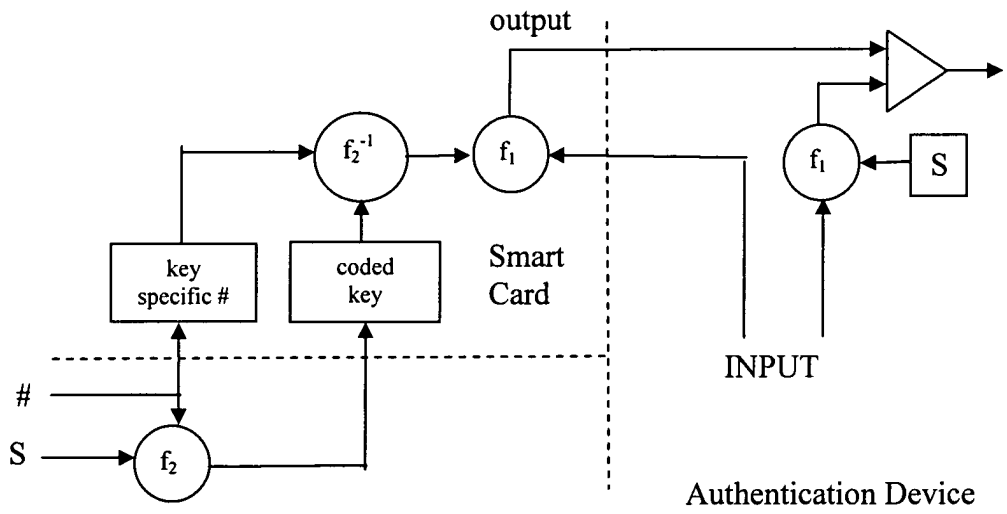
After the foregoing Amendment, claims 9-16, as amended, are pending in this application. Claims 1-8 have been canceled.

Rejection - 35 U.S.C. § 103

The Examiner rejected claims 9, 10, 12, and 14-16 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 4,471,216 (Herve) and U.S. Patent No. 5,604,810 (Dolan et al.).

The Present Invention

The fundamental operation of the present invention for producing a response from the smart card is illustrated by the following figure, based on the second preferred embodiment, onto which claims 9-16 read.



Note: rectangular boxes denote device memory and contents thereof.

In the second preferred embodiment of the invention, an authentication device stores a secret key "S". The smart card stores in it's memory, a coded version of the secret key, S, and a key specific number. The secret key is coded with a function f_2 using the key specific number as a key encryption key.

When the smart card is connected to the authentication device for the purpose of generating a response, an INPUT, generated by the authentication device, is input to the smart card. The smart card decodes the coded key stored in the smart card using an inverse of the function f_2 and the stored key-specific number and then uses the decode of the coded key (i.e. the secret key, S) as the key for coding the INPUT. The coded INPUT is then output to the authentication device. The authentication device, more or less simultaneously, uses the secret key, S, stored in the authentication device to code the INPUT using the function f_1 to form a check value and compares the output of the smart card with the check value. If the output and the check value are identical, the smart card is authenticated.

The Examiner takes the position that Herve teaches a method of producing a response with a device comprising an input for receiving an input, calculation means for producing a response which is responsive to the input and a secret key by utilizing a first predetermined function. The Examiner further suggests that the Dolan *et al.* patent teaches the features of the claims not taught by Herve, namely, storing in a memory of the device a key-specific number and a coded key which is calculated by means of a secret key, the key-specific number and a device-specific second predetermined function, and when producing the response, reading the key-specific and the coded key from the memory, calculating the secret key on the basis of the key-specific number and a coded key by using the inverse function of the second predetermined function and utilizing the calculated secret key to produce the response. The Examiner concludes that it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Dolan *et al.* into the system of Herve and that motivation to make the combination is found in column 2, lines 10-40 of Dolan *et al.* For the reasons set forth in detail below, the Applicant respectfully traverses the rejection as applied to claims 9, 10, 12, and 14-16.

Claim 9 recites:

A method of producing a response with a smart card, the smart card comprising:

an input for receiving an INPUT;

calculation means for producing a response which is responsive to the INPUT and a secret key by utilizing a first predetermined function; and

an output for outputting said response;

said method comprising:

storing in a memory of the smart card a key-specific number and a coded key, which has been calculated using the secret key, the key-specific number and a second predetermined function; and,

when producing the response:

reading said key-specific number and said coded key from the memory of the smart card;

calculating the secret key with the smart card using said key-specific number and said coded key by using the inverse function of said second pre-determined function; and

utilizing the calculated secret key, the INPUT and the first predetermined function to produce said response with said smart card.

Herve discloses a portable object useful for access control. The portable object includes a memory. The memory stores a secret key and an ID code. In use, as described at col. 3, lines 11-24, the ID code is provided to an authentication device by the portable object. The authentication device has a copy of the secret key. If the ID code is plausible, the authentication device generates a random number which is input to the portable object. The portable object generates a number R as a function of the ID code, the secret key and the random number and

transmits the number R to the authentication device. If the number R is identical to a number generated in the authentication device based on the secret key, the random number and the ID code, the portable object is authenticated.

The method disclosed by Herve is different from the method recited in claim 9. Herve stores the secret key in the smart card. In contrast, claim 9 recites storing a coded key in the smart card, where the coded key is calculated from the secret key with a second function. Significantly, the secret key is not stored in the smart card of the present invention and thus is not subject to unauthorized use. Further, claim 9 recites calculating the secret key from the coded key with an inverse of the second function, while the portable object of Herve has no equivalent step. Claim 9 also recites generating the response using the calculated secret key and a first function. Again, Herve has no equivalent step.

Dolan et al. discloses a communication system comprising one or more portable devices and a server. The server stores an encrypted version of a private (secret) key unique to each portable device or group of portable devices. Each portable device stores one or more numbers which are used for encrypting a hash of an unencrypted message. Dolan et al. discloses a first embodiment, an enhanced first embodiment and a second embodiment. In each of the embodiments the unencrypted message is transmitted from the portable device to the server. A digital signature is attached to the message by: (1) hashing the message in the portable device, (2) encrypting a key encryption key (KEK) in the portable device using the hashed message as key; (3) decrypting the KEK in the server using the hash of the message received in the server; (4) decrypting the encrypted private in the server using the decrypted KEK and (5) encrypting the unencrypted message received in the server using the decrypted private key.

The structure and the operation of Dolan et al. is substantially different from the present invention. Dolan et al. describes a system for attaching a digital signature to an unencrypted message using the well known technique of generating a hash of the message to create a key for generating the digital signature. Authentication is performed by comparing the hash of the unencrypted message transmitted from the portable device to the server with a hash of the unencrypted message received by the server. In contrast, the present invention transmits a coded version of a secret key from a smart card to a device, where the device authenticates the

smart card by directly comparing the coded key transmitted from the smart card with a coded version of the secret key stored in the authentication device.

More importantly, Dolan et al. does not teach, suggest or disclose those features of claim 9 which Herve lacks.

1. The Examiner states that Dolan et al. teaches storing in a memory a key-specific number, a coded key which is calculated by means of a secret key, a key specific number and a device specific second predetermined function, as described at col. 3, line 65 to col. 4, line 18.

The description at cols. 7-8 refers to a KEK as a reversible function of a password or PIN. Only the first enhanced embodiment described at col. 7 starting a line 25, and Figs. 5-6, and the second embodiment described starting at col. 8, line 39 and Figs. 7-9 disclose a PIN.

In the first enhanced embodiment, the PIN is used to generate a number PKREVa as the "exclusive or" (XOR) of the PIN and a hash of the secret key SKa (KOWFa). The number PKREVa is then XORed with the PIN to generate a key KOWFa for encrypting the transient key encryption key (KEK). The number PKREVa and the hash of the PIN are stored in the memory of the portable security device (see Fig. 5). Clearly, of the PIN, KOWFa, and PKREVa, only PKREVa can be equated with the key-specific number stored in the memory of the smart card, since of the PIN, KOWFA and PKREVa, only PKREVa is stored in the memory of the portable device. Further, the PIN is related to the user and is not specific to the key.

Referring to cols. 3-4 and 7-8, it appears that the Examiner must be equating the KOWFa with the claimed coded key, PKREVa with the key-specific number and the XOR function with the claimed second predetermined function (as he must to satisfy the limitations of claim 9). Consequently, one must equate the PIN to the user's secret key in order to satisfy claim 9. However, Dolan et al. clearly distinguishes between the secret key SKa and the PIN and thus it is improper to equate the PIN with the secret key. Further, Dolan does not disclose in the first enhanced embodiment storing KOWFa in the portable device. Accordingly, Dolan et al. does not disclose storing in a smart card a coded key which is calculated by means of a secret key, a key specific number and a device specific second predetermined function, as recited in claim 9.

In the second embodiment, a PIN is used merely to authenticate the user by comparing a hash of the PIN with a stored hash of the PIN. There is no disclosure of generating a KEK as a reversible function of the PIN and thus no disclosure of storing in a memory of the smart card a key-specific number, and a coded key which has been calculated from the secret key, the key specific number and a second predetermined function, as recited in claim 9.

2. The Examiner further states at col. 4, lines 1-11, that Dolan et al. calculates the secret key on the basis of the key-specific number and coded key using an inverse of the second predetermined number. However, Dolan et al. never calculates the secret key SKa in the portable device. Accordingly, Dolan et al. does not disclose a calculated secret key to generate an output from the portable device, as recited in claim 9.

To establish *prima facie* obviousness of a claimed invention, all the claimed limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974), MPEP §2143.03.

Because neither Herve nor Dolan et al. teach, suggest or disclose the above identified limitations of claim 9, the combination of Herve and Dolan et al. can not possibly teach or suggest all the limitations of claim 9.

Applicant further submits that Herve and Dolan et al. are not properly combinable under 35 U.S.C. § 103. There is no teaching, suggestion or disclosure in Herve et al. to store a coded key in the portable object or to calculate the secret key in the portable object from a coded key stored in the portable object. Further, the storing of a coded key in place of the secret key would not materially change the operation of the system disclosed by Herve, since whether or not the key was coded would make no difference to the system operation as long as the secret key in the facility were also coded. Nor would it increase the security of the key. This is because the operation of the system disclosed by Herve is independent of the number stored in the portable object as long as the same number is stored in the facility. Accordingly, there would be no motivation to change the operation of Herve to store a coded key. Also, if a coded key were used in the portable object without the same key being stored in the facility, the design of the entire system would have to be impermissibly changed.

Further, there is no teaching or suggestion in Dolan et al. to adopt the technique of

transmitting the encrypted secret key from the portable device to the server. Further, there would be no motivation to transmit the encrypted secret key since that would not accomplish the objective of providing a digital signature.

Accordingly, for all the above reasons, Applicant respectfully requests reconsideration and withdrawal of the §103 rejection of claim 9.

Further, it is respectfully submitted that since claim 9 has been shown to be allowable, claim 10, dependent on claim 9 is allowable, at least by its dependency. Accordingly, for all the above reasons, Applicant respectfully requests reconsideration and withdrawal of the § 103 rejection of claim 10.

Claims 12 and 14 each recite, *inter alia*, a smart card comprising a memory for storing a coded key which has been calculated using a second predetermined function and means for calculating a secret key by means of the coded key and an inverse of the second predetermined function. As discussed above, neither Herve nor Dolan et al. teach the aforementioned limitations. Accordingly, for the same reasons as for claim 9, Applicant respectfully requests reconsideration and withdrawal of the §103 rejection of claims 10 and 14.

Further, it is respectfully submitted that since claim 14 has been shown to be allowable, claims 15 and 16 , dependent on claim 14 are allowable, at least by their dependency. Accordingly, for all the above reasons, Applicant respectfully requests reconsideration and withdrawal of the § 103 rejection of claims 15 and 16.

Rejection - 35 U.S.C. § 103

The Examiner rejected claims 11 and 13 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 4,471,216 (Herve) and U.S. Patent No. 5,604,810 (Dolan et al.) and further in view of WO 99/35782 (Kocher).

As discussed above, neither Herve nor Dolan et al. teach or suggest storing a coded key in a memory of a smart card or calculating the secret key in the smart card with an inverse of the key used to generate the coded key, and using the calculated secret key to generate a response, as recited in claims 9 and 12. Claims 11 and 13 depend respectively from claims 9 and 12. Kocher fails to make up for the deficiencies of Herve and Dolan et al. Accordingly,

Applicant respectfully requests reconsideration and withdrawal of the § 103 rejection of claims 11 and 13.

PTO 982

The Examiner has cited U.S. Patent No. 4,471,216 (Herve) as prior art but has failed to list Herve on a PTO-892 form. Applicant respectfully requests that the reference to Herve be listed on a PTO-892 form so that the reference will appear on the face of the patent when issued.

CONCLUSION

Insofar as the Examiner's rejections have been addressed, the application is in condition for allowance and Notice of Allowability of claims 9-16 is therefore earnestly solicited. Should the Examiner choose to issue an advisory action, Applicant respectfully requests that prior thereto, the Examiner telephone the undersigned at the telephone number indicated to discuss the application.

Respectfully submitted,

LAURI PAATERO

January 9, 2006 By: _____
(Date)

LOUIS SICKLES II
Registration No. 45,803
AKIN GUMP STRAUSS HAUER & FELD LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1200
Direct Dial: 215-965-1294
Facsimile: 215-965-1210
E-Mail: lsickles@akingump.com

LS